Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Modelování počítačové sítě pomocí nástroje GNS3

Modelling of Computer Network Using GNS3 Tool

2013 **Lukáš Czakan**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Lukáš Czakan**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Modelování počítačové sítě pomocí nástroje GNS3
Modelling of Computer Network Using GNS3 Tool

Zásady pro vypracování:

1. Proveďte analýzu vlastností nástroje GNS3.
2. Pomocí nástroje GNS3 vytvořte simulaci komplexní architektury počítačové sítě.
3. Celý postup zdokumentujte a vytvořte 2 zadání pro laboratorní cvičení odborného předmětu.

Seznam doporučené odborné literatury:

Graphical Network Simulator. *GNS3* [online]. [cit. 2012-11-08]. Dostupné z: http://www.gns3.net/

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Libor Michalek, Ph.D.**

Datum zadání: 01.09.2013

Datum odevzdání: 07.05.2014

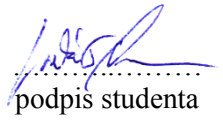
doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *29. dubna 2014*



.....
podpis studenta

Poděkování

Rád bych poděkoval panu Ing. Liboru Michalkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Abstrakt

Cílem této práce je analyzovat vlastnosti nástroje GNS3 a vytvořit simulaci komplexní architektury počítačové sítě. Na základě této simulace vytvořit 2 zadání pro laboratorní cvičení z odborného předmětu.

Při tvorbě této práce budu používat software GNS3 ve verzi 0.8.6, který je v neustálém vývoji a předpokládám, že v době představení mé práce bude k dispozici i v novější verzi. Chtěl bych čtenáře seznámit s výhodami a možnostmi nástroje GNS3 a předvést mu praktickou realizaci konkrétní architektury počítačové sítě. Dále bych chtěl vytvořit dvě plnohodnotná cvičení pro odborný předmět, ve kterých si žáci vyzkouší, jak práci s nástrojem GNS3, tak konfiguraci prvků poskytovaných nástrojem a aplikaci dosavadních znalostí počítačových sítí.

Klíčová slova

GNS3; IOS; IOS obraz, aktivní plátno, směrovač, přepínač, virtuální stroj, konfigurace

Abstract

The aim of this work is to analyze the characteristics of the GNS3 tool and create a simulation of a complex network architecture. Based on this simulation to create two tasks for laboratory exercises in vocational subject. In creating this work, I will use GNS3 software in version 0.8.6, which is still in constant evolution and i suppose, that the later versions will be avaliable in time of my presentation. I would like to acquaint the readers with benefits and possibilities of the GNS3 tool and show them the practical implementation of the specific network architecture. Furthermore, I would also like to create two full tasks for vocational subject in which students will try to work with the GNS3 tool and also try configuration features provided by the tool and the application of existing knowledge of computer networks.

Key words

GNS3; IOS; IOS image, active canvas, router, switch, virtual machine, configuration

Seznam použitých zkratek

Zkratka	Význam
GNS3	Graphical Network Simulator
RAM	Random Access Memory
WIC	WAN Interface Card
NVRAM	Non-volatile Random Access Memory
IOS	Internetwork Operating System
VPCS	Virtual PC Simulator
RTP	Real-time Transport Protocol
TCP	Transmission Control Protocol
VOIP	Voice Over IP
WIC	WAN Interface Card

Seznam použitých termínů

Termín	Význam termínu
Putty	Terminál
WinPCAP	Knihovna umožňující přistup k síti a k síťovým zařízením
Wireshark	Protokolový analyzér a packetový sběrač
Qemu	Terminál
Pemu	Terminál
VirtualBox	Software umožňující virtualizaci operačních systémů
VMWare	Software umožňující virtualizaci operačních systémů
Virtual PC	Virtuální počítač VPCS, který je součástí GNS3
Dynamips	Jádro programu GNS3
Dynagen	Textový výstup programu Dynamips
NVRAM	Pamět, která si uchová data i když je vypnuto napájení

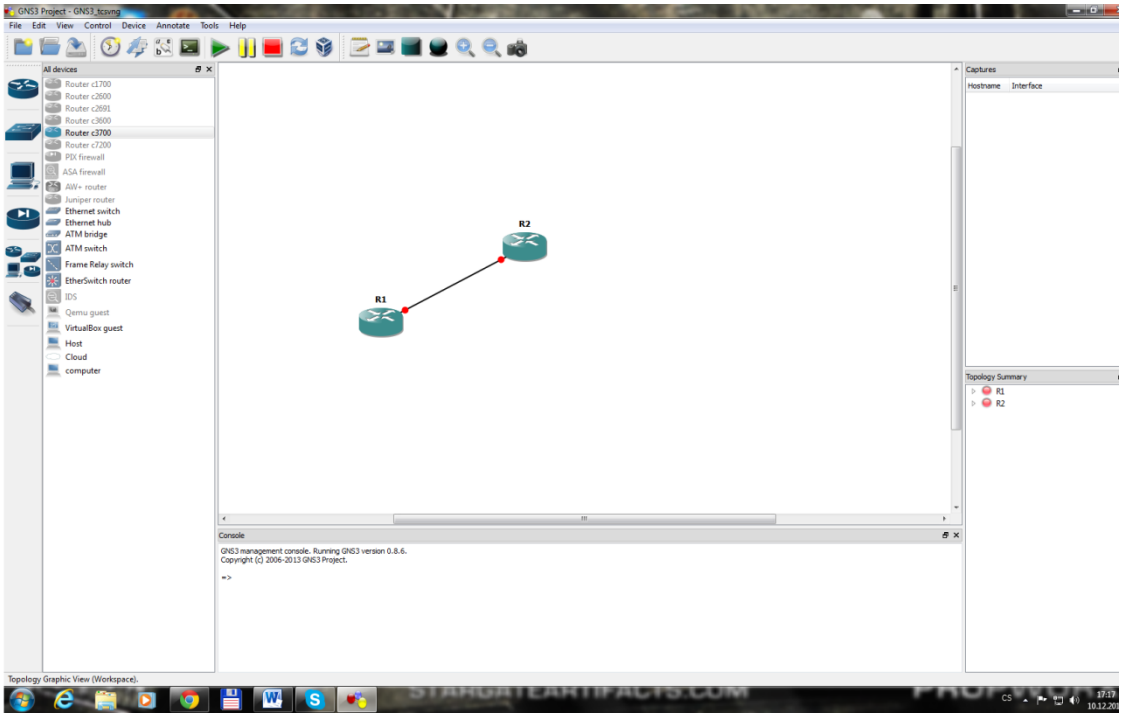
Obsah

Úvod

Dobrý den vážení čtenáři, už jste se možná dostali do situace, kdy jste se chtěli prakticky vzdělávat v oblasti počítačových sítí, ať již z osobního zájmu nebo v rámci požadavků vaší práce, školy, ale z důvodu vysokých cen síťových zařízení, jste nemohli okusit všechny možnosti. Při mém studiu počítačových sítí jsem se dozvěděl mnoho užitečných informací a při práci v perfektně vybavených laboratořích mé vysoké školy jsem dosáhl i širokého repertoáru praktických dovedností. Přece jen jsem nebyl schopen v praktických hodinách pochytit to obrovské množství informací za pár lekcí. Z tohoto důvodu jsem hledal možnosti, jak bych mohl nabyté znalosti otestovat a studovat sám na svém osobním počítači bez utrácení peněz za zařízení. První nástroj, který jsem začal používat, byl Packet Tracer od společnosti CISCO. V programu jsem mohl odzkoušet všechno, co jsem se naučil. Byla to pouze simulace a neviděl jsem ovoce své práce v reálném čase. Všechno se změnilo, když jsem si vybral své zadání Bakalářské práce. Začal jsem se seznamovat s nástrojem GNS3 a byl jsem velice překvapen. Tento nástroj na rozdíl od jiných funguje nejen jako simulace, ale také jako emulace opravdových reálných zařízení za desítky tisíc korun a to v reálném čase. Díky tomuto nástroji si můžu doma reálně sestavit téměř jakoukoli síťovou situaci a sledovat, jak se chová. Dokonce si můžu zachytávat aktuální provoz díky integraci programu Wireshark sloužícímu k monitoringu provozu na síťovém rozhraní a mnoha dalším funkcím, o kterých se zmíním v této práci.

1 Úvod do GNS3

GNS3 (Graphical Network Simulator) je grafický síťový simulátor, který umožňuje emulování komplexních počítačových sítí. GNS3 pracuje ve virtuálním prostředí, jako například známe programy VirtualBox, VMWare nebo Virtual PC emulující operační systémy Linux, Windows XP, Windows 7, Mac-OS X. Na rozdíl od zmíněných programů, však emuluje Cisco Internetwork Operating Systems známé jako Cisco IOS, což jsou vlastně operační systémy síťových zařízení společnosti Cisco, ale také JunOS od konkurenční firmy Juniper. Jádrem nástroje GNS3 je program Dynamips, který nám právě tuto emulaci umožňuje.



Obrázek 1.1: *Grafické prostředí GNS3*

Dá se říci, že program GNS3 je vlastně grafická nadstavba programu Dynamips umožňující uživateli příjemnější ovládání. GNS3 rovněž podporuje ostatní emulační programy jako VirtualBox, Qemu, Pemu. Tyto programy jsou v GNS3 využívány k emulaci počítačových hostů (Linux, Windows, atd.), emulaci Cisco přístupových bodů ASA, emulaci Cisco PIX (Private Internet eXchange) firewallu a nebo emulaci systémů pro prevenci průniku Cisco IPS. GNS3 umí emulovat IOS na routeru společně s operačním systémem Windows na hostitelském PC najednou a umožní jejich vzájemnou komunikaci.

GNS3 lze spustit na vašem počítači s podporou operačních systémů Windows, Linux, Mac-OS X. GNS3 podporuje emulaci velkého množství hardwaru od společnosti Cisco, což z něj dělá vynikající nástroj pro přípravu na certifikáty jako třeba CCNA, CCNP a CCIE. Úplný

seznam podporovaného hardwaru naleznete v příloze číslo 1 "Seznam podporovaného hardwaru" nebo na stránkách programu GNS3 [1].

Existuje celá řada simulátorů routerů, ale jejich možnosti jsou omezené. Zpravidla neumožňují využívat všechny příkazy daného hardwaru nýbrž jen ty, které poskytne vývojář tohoto simulátoru. GNS3 naproti tomu není limitován ničím. Na routeru je spuštěn IOS daného typu a uživatel vidí naprosto přesně, co se zrovna v zařízení děje. Množství příkazů je omezeno pouze verzí IOS.

GNS3 je distribuován jako freeware, což znamená, že je dostupný zcela zdarma. Je však třeba být vlastníkem Cisco IOS obrazu, který se nahraje jako systém pro daný router.

I když nám tento software přináší téměř neomezené možnosti při práci se síťovými prvky, je nutné si uvědomit, že je to software určený pro vzdělávání a pro testování v laboratořích. Virtuální prostředí nástroje GNS3 umožňuje propustnost kolem 1000 packetů za sekundu, kdežto normální router 100x až 1000x víc. Další informace se lze dočíst ve [6].

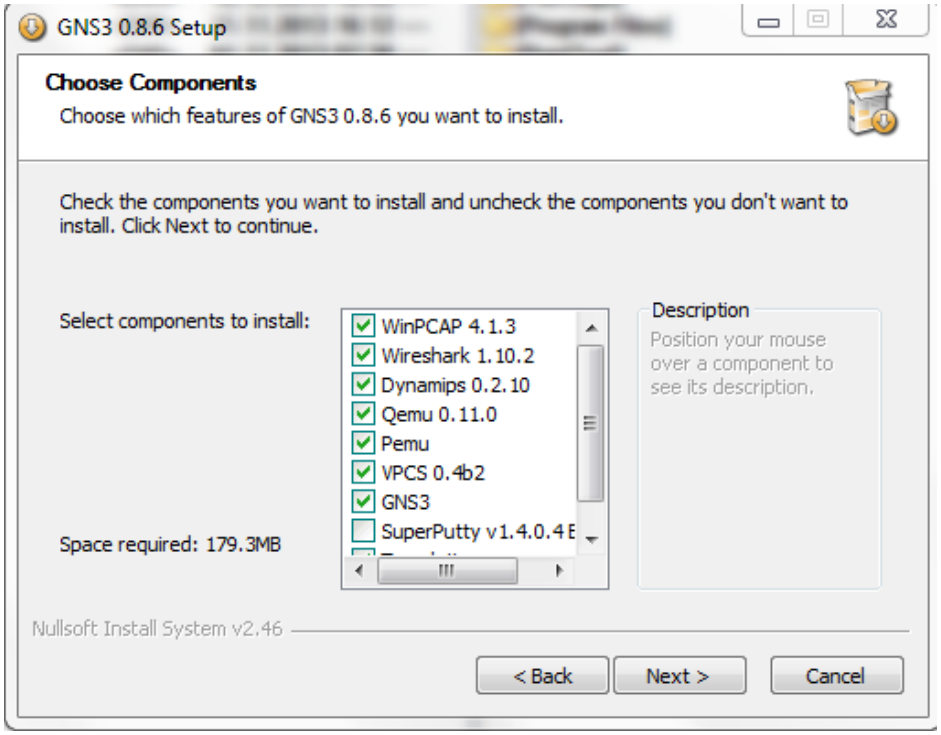
1.1 Instalace GNS3

Nástroj GNS3 lze nainstalovat na počítače s operačními systémy Windows, Linux, Mac-OS. V této práci uvádím krátký návod pro jednoduchou instalaci na nejběžněji používaných systémech Windows a Linux.

1.1.1 Instalace pro Windows

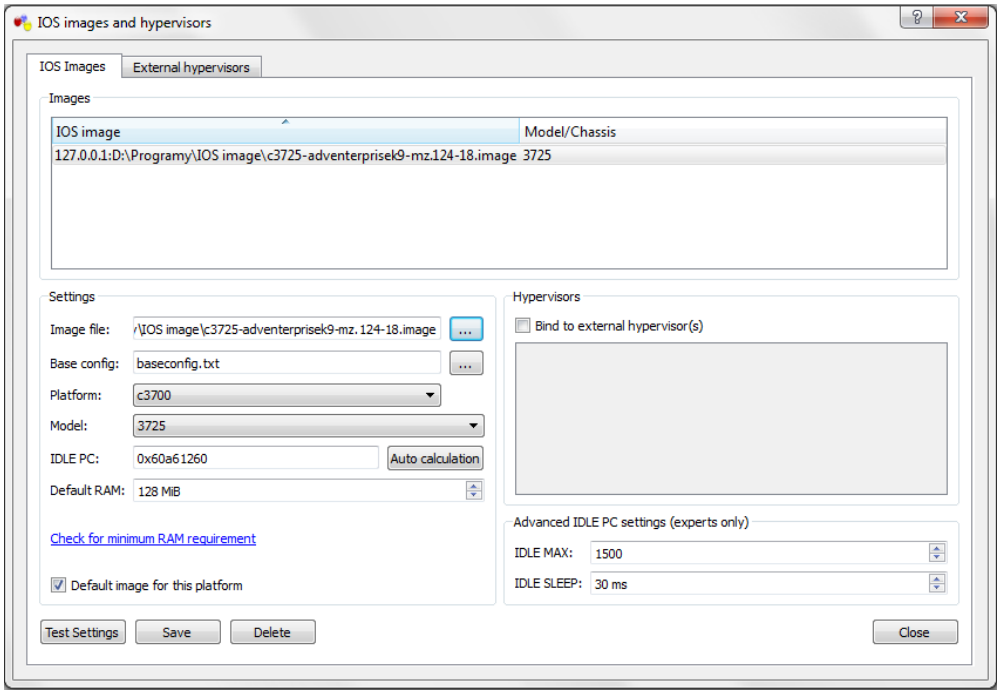
Nejprve je třeba program stáhnout. Lze jej stáhnout přímo z oficiálních webových stránek GNS3. Nejjednodušší je stáhnout "All - in - one " balíček, který obsahuje instalátor pro 32 bitové a 64 bitové operační systémy, Dynamips, Qemu/Pemu, Putty, VPCS, WinPCAP a Wireshark. Velikost balíčku je zhruba 60 MB.

Kliknutím na stažený balíček spustíme instalačního průvodce. V instalačním průvodci se pohybujeme stiskem tlačítek **NEXT/BACK** nebo **AGREE**. GNS3 instalace závisí na instalaci důležitých komponent výše zmíněných. Zatržením si zvolíme, zdali chceme komponentu nainstalovat nebo odtržením, když ji již nainstalovanou máme. V případě neaktuální komponenty se instalátor dotáže, zda chceme odinstalovat původní verzi a nainstalovat aktuální.



Obrázek 1.2: *Průvodce instalací*

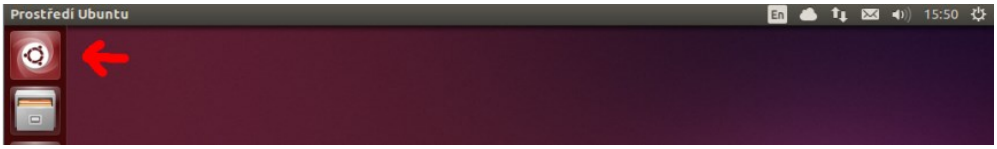
Nyní máme nainstalován GNS3. Spustíme program z nabídky Start nebo z adresáře, kde byl nainstalován. Otevře se hlavní okno rozdělené do 4 částí. Jednotlivé části jsou popsány v kapitole Grafické uživatelské rozhraní. Nyní přidáme IOS obraz do GNS3. Klikneme na položku **EDIT** a vybereme **IOS images and hypervisors**. Pod záložkou **Image file** klikneme pro výběr a zvolíme námi vlastněný IOS obraz. Obraz se nám zobrazí v poli. Dále klikneme na rozbalovací menu u záložky **Platform** a vybereme typ platformy odpovídající našemu IOS obrazu. Nyní rozbalíme rozbalovací menu pod záložkou "Model" a vybereme model routeru odpovídající vlastněnému IOS obrazu. Dále můžeme libovolně nastavit hodnotu paměti RAM, kterou chceme vymezit pro náš IOS, a to v poli **Default RAM**. Velmi důležitá je záložka IDLE PC, která nám umožňuje optimalizovat vytížení procesoru. Podrobněji o IDLE PC se zmiňuji v kapitole Optimalizace, proto tuto hodnotu zatím nevyplňujeme.



Obrázek 1.3: *Načtení IOS obrazu a počáteční nastavení*

1.1.2 Instalace pro Linux

Pro Ubuntu verze, které jsou starší než verze 11.10, otevřeme Synaptic Package Manager, který nalezneme v **System Menu > Administrations > Synaptic Package Manager**. Pro novější verze Ubuntu stačí spustit Ubuntu Software Center, který lze nalézt nejčastěji v levém panelu.



Obrázek 1.4: *Ubuntu Software Center*

Jednoduše vyhledáme GNS3. Když jej nalezneme, klikneme na tlačítko Install. Ubuntu stáhne GNS3 a všechny s ním související rekvizity, zároveň se spustí instalátor GNS3. Navigace v instalátoru je potom stejná jako v případě instalace pro Windows.

1.2 Začínáme v GNS3

Při prvním spuštění je třeba nejen provézt několik nutných kroků, které byly zmíněny v kapitole Instalace GNS3, ale také se seznámit se základním rozvržením Grafického uživatelského rozhraní, s možnostmi přidávání prvků na aktivní plátno, s optimalizací vytížení procesoru a dalšími základními vlastnostmi nástroje GNS3.

1.2.1 Grafické uživatelské rozhraní

Grafické uživatelské rozhraní je rozděleno do čtyř větších oken, horního pásu ikon, levého pásu ikon a horní lišty. Levý pás ikon obsahuje schválené ikony skupin síťových prvků jako jsou routery, switche, koncová zařízení, bezpečnostní prvky, všechny prvky a ikonu pro vytvoření spoje. Hned vedle levého pásu ikon je první okno zobrazující dostupné prvky ve skupině, která je právě vybrána. Když například vybereme skupinu routerů, zobrazí se nám v tomto okně seznam všech dostupných routerů, pro které máme instalován IOS obraz. Jsou zobrazeny i routery, pro které obraz instalován není, ale nelze s nimi nijak manipulovat.

Uprostřed a nahoře máme další okno. Toto okno je pro uživatele nejdůležitější, jelikož se jedná o aktivní plátno, kde lze libovolné prvky přetahovat, spojovat, spravovat a vidíme jejich grafickou reprezentaci. Umožňuje nám vidět i stavy jednotlivých rozhraní (aktivní / neaktivní). Můžeme si do něj dělat poznámky, kreslit hraniční tvary atd.

Hned pod aktivním plátnem je okno pro konzoli. Jedná se o konzoli Dynagenu, což je textový vstup a výstup programu Dynamips. Zobrazuje nám Dynagen při práci. Během práce v GNS3 poskytuje výpisy o stavu Dynamips a jeho procesech.

Úplně napravo je okno rozdělené do dvou částí. První a horní část obsahuje výpis zachyceného provozu v námi vytvořené síťi. Druhá a spodní část nám zobrazuje sumarizaci všech prvků umístěných na aktivním plátně. Signalizuje jejich stav a po rozbalení určitého prvku i popis jejich rozhraní, a kam jsou napojena.

Horní pás ikon obsahuje základní ikony symbolizující řídící operace. Ikony jsou intuitivní a na první pohled lze odhadnout, k čemu jsou určeny. Obsahují například ikonu pro vytvoření nového projektu, uložení projektu, zapnutí a vypnutí všech prvků na aktivním plátně, přechod do konfigurační konzole prvku, ikonu pro vytvoření poznámky, přidání obrázku, přidání tvaru, vytvoření screenu aktivního plátna, zobrazení popisů rozhraní či spuštění VirtualBoxu.

Obrázek 1.5: *Horní pás ikon*

Horní lišta je tvořena klíčovými tlačítky. Jsou to klasická rozbalovací tlačítka, jejichž názvy vypovídají o tom, jaké funkce budou poskytovat. Jsou to tlačítka File, Edit, View, Control, Device, Annotate, Tools, Help.

1.2.2 První router

Všechny prvky v GNS3 vybíráme z levého okna vedle levého pásu zobrazujícího skupiny zařízení. Router vybereme kliknutím na skupinu routerů. Otevře se nám levé okno s nabídkou všech podporovaných routerů. Router přetáhneme na aktivní plátno a kliknutím umístíme. Přetahovat lze jen routery, které mají instalován IOS o dané verzi. Po přetáhnutí routeru na aktivní plátno se nám zároveň objeví značka v okně pro sumarizaci prvků.

Dvojklikem na daný router se dostaneme do konfigurace routeru. Lze vidět obecný popis zařízení, jeho obrazu a počáteční konfigurace. Můžeme měnit velikost paměti RAM poskytnuté systémem pro tento router. Další možností je přidání až sedmi slotů pro adaptéry a až tři sloty pro síťové karty WIC (WAN Interface Card). Popis jednotlivých síťových modulů pro IOS c3725 je uveden v příloze Seznam podporovaného hardwaru. Router spustíme pravým kliknutím a výběrem možnosti Start. Tato operace chvíli trvá v závislosti na výkonnosti systému, na kterém je emulace spouštěna. Se spuštěným routerem můžeme provádět další řadu operací, jako například změnit symbol, změnit port pro konzoli apod. Nejdůležitější je však funkce terminálu. Spustíme jí výběrem funkce Console. Zobrazí se nám okno terminálu, ve kterém vidíme, jak router nabíhá a bootuje svůj systém. Jelikož se jedná o emulaci, toto nabíhání může trvat tak dlouho, jako u reálných routerů. Pokud nám terminál nevyhovuje, můžeme je změnit za jiný. Po doporučené instalaci na systému Windows je automaticky nastaven terminál Putty, ale GNS3 podporuje i terminály SecureCRT, SuperPutty, Telnet, Xshell 4, TeraTerm nebo TeraTerm Pro. Změnu terminálu provedeme v záložce Edit > Preferences > General, a tam zvolíme Terminal Settings.

1.2.3 Optimalizace

1.2.3.1 Idle PC

Jádrem nástroje GNS3 je program Dynamips. Spuštěný router využívá téměř všechen výpočetní výkon procesoru, i když zrovna neprodukuje žádný provoz. Dynamips je emulátor a jako takový načítá každou instrukci z binárního obrazu strojového kódu a okamžitě ji provádí na hostitelském počítači pořád dokola. Proto v GNS3 existuje funkce nazvaná Idle PC. Tato funkce zamezí neustálé inkrementaci strojového kódu nastavením hodnoty Idle PC value. Tato hodnota vymezuje smyčku, při které budou znovu provedeny všechny instrukce, a tudíž nebudou opakovány pořád dokola, ale jen jednou za určitý čas. Toto nám umožňuje výrazně snížit vytížení procesoru počítače a zároveň nezmrazí daný router, takže si může průběžně dělat, co potřebuje (výpisy apod.). Pro kalkulaci Idle PC hodnoty musí být router aktivní. GNS3 chvíli počítá a poté nabídne seznam doporučených hodnot Idle PC value. Nejoptimálnější hodnota je zvýrazněna hvězdou.Více o této tématice se můžete dočíst na uvedeném odkazu [5].

1.2.3.2 Ghost IOS

Komplexní topologie mohou zabírat velké množství paměti počítače, na kterém je spuštěn GNS3. Tento problém řeší funkce Ghost IOS. V normálním případě každý router se stejným IOS obrazem ukládá identickou kopii IOSu do virtuální paměti RAM hostitelského

počítače. Se zapnutou funkcí Ghost IOS hostitelský počítač alokuje takzvaný sdílený region virtuální paměti RAM s jedním obrazem IOSu, který je využíván všemi routery.

1.2.3.3 ***Sparesmem***

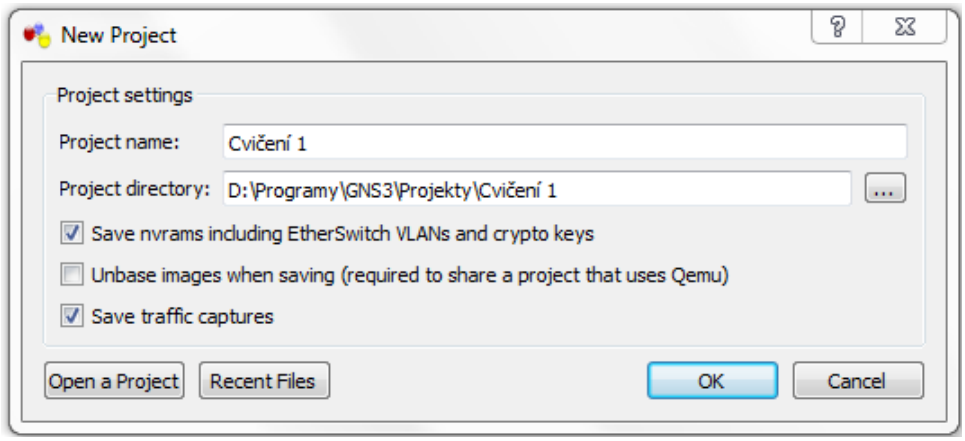
Další optimalizační funkcí je Sparesmem. Tato funkce nešetří skutečnou RAM paměť hostitelského počítače, ale místo toho snižuje množství virtuální paměti používané emulovaným routerem.

2 Komplexní architektura počítačové sítě

2.1 Cvičení číslo 1

2.1.1 Základní dovednosti v GNS3

1. Spustíme program GNS3. Jako první se nám objeví dialogové okno New Project. Vytvoříme si tedy nový projekt se specifickým názvem a zvolíme uložiště našeho projektu. Zvolíme uložit paměti NVRAM obsahující konfigurace VLANů Ethernetových switchů a kryptografické klíče. NVRAM (Non-volatile Random Access Memory) paměť je koncipována podobně jako paměť RAM s tím rozdílem, že si své informace uchovává i po vypnutí napájení. Jelikož budeme používat program Wireshark, který je integrován do GNS3, uložíme si také veškerý provoz jím zachycený. Jelikož v našem projektu nebudeme používat Qemu terminály, tak druhou položku necháme volnou.



Obrázek 2.1: *Nový projekt*

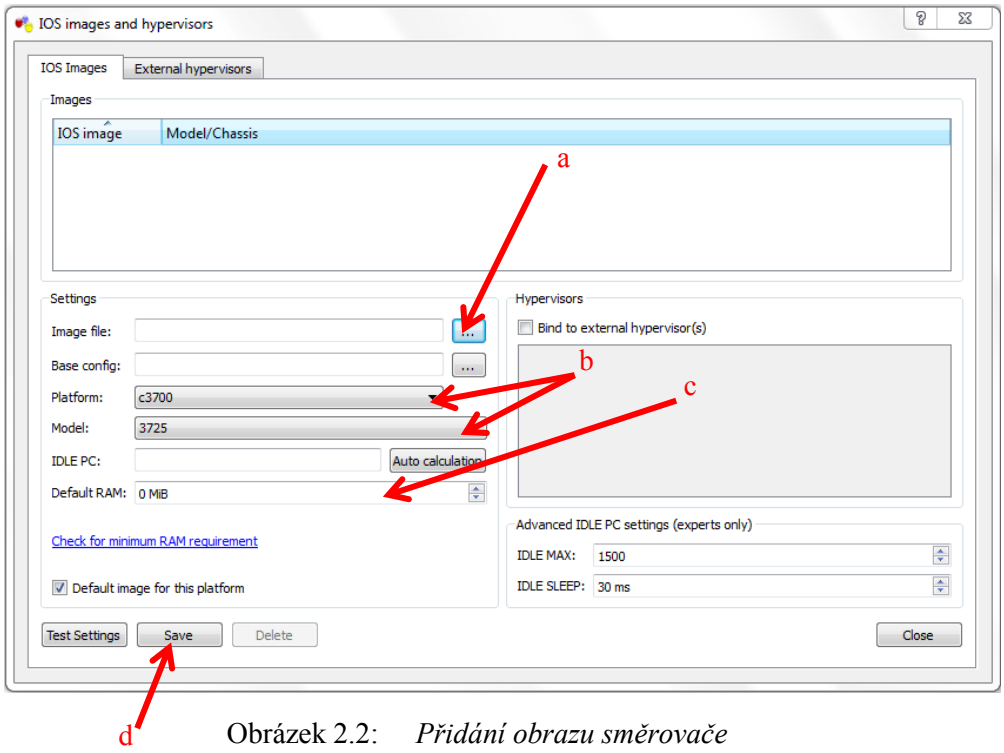
2. Abychom mohli využít plný potenciál systému GNS3, tak je nutné naimportovat obraz systému routeru (v našem případě IOS). Přejděme tedy na položku Edit a vybereme položku IOS images and hypervisors.

a) vybereme soubor s obrazem IOS

b) náš obraz je platformy 3700 model 3725

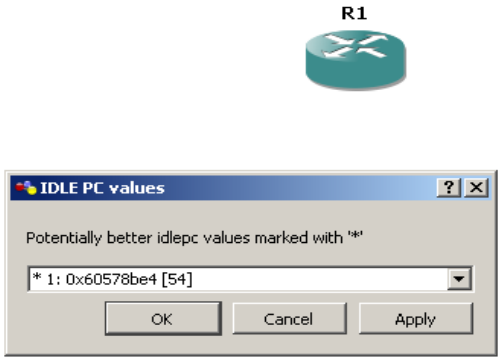
c) výchozí RAM nastavíme na 128 MiB

d) uložíme nastavení



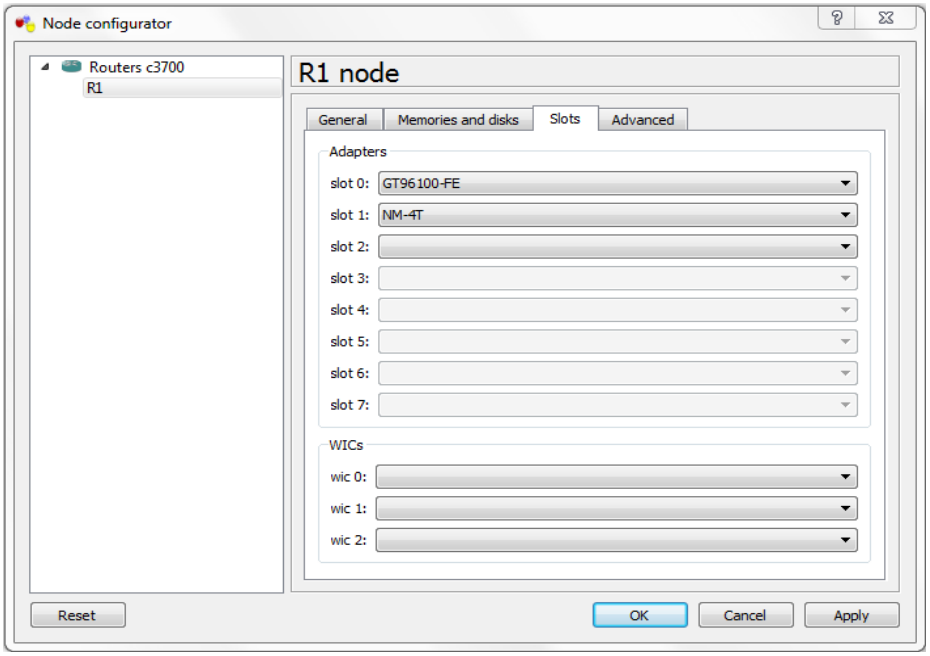
Obrázek 2.2: *Přidání obrazu směrovače*

3. Nyní rozbalíme z levého pásu ikonu směrovače a náš model přetáhneme na aktivní plátno (pokud nemáte aktivovány další obrazy, náš bude jediný, který bude zabarvený). Klikneme pravým tlačítkem myši a spustíme směrovač možností Start. Jelikož takto spuštěný směrovač ještě není plně optimalizován a využíval by nadbytečně mnoho výkonu, použijeme možnost Idle PC. Systém GNS3 bude chvíli počítat nejlepší hodnotu Idle PC, a poté nám dá na výběr z několika hodnot, přičemž nejlepší hodnota je označena hvězdičkou. Zvolíme některou z hodnot a potvrdíme stiskem tlačítka Apply.



Obrázek 2.3: *Idle PC hodnota*

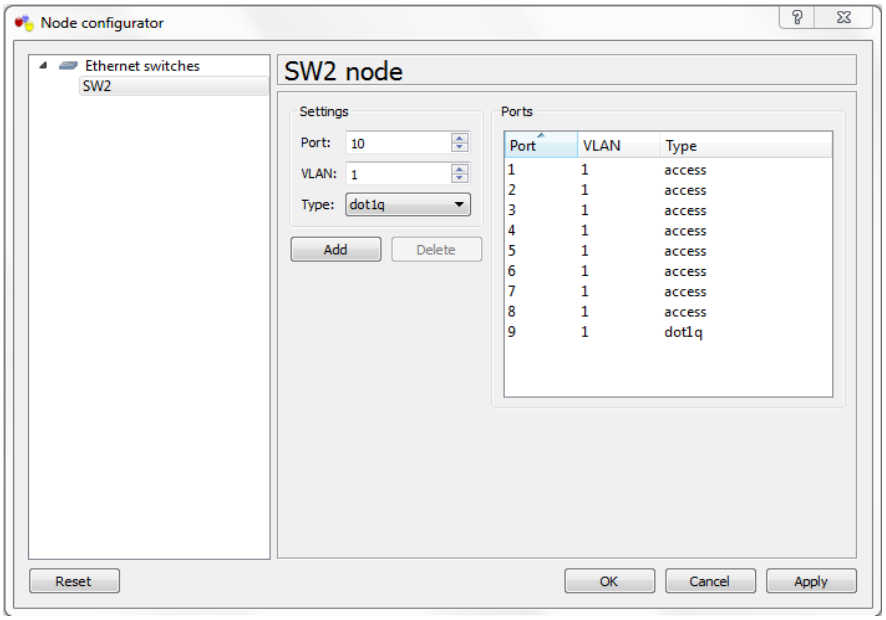
4. Nyní chceme používat sériové rozhraní našeho routeru, a proto jej musíme přiřadit do volného slotu. To provedeme pravým kliknutím a vybráním položky Configure. V záložce Slots je na pozici slot0 defaultní adaptér pro 2x Fast Ethernet GT96100. My chceme používat i sériové rozhraní, a tudíž do volného slotu vybereme adaptér NM-4T se 4 sériovými porty. Toto nastavení se dá aplikovat i na celou skupinu routerů c3700.



Obrázek 2.4: *Přídavné sloty*

5. Teď když už můžeme používat sériové rozhraní, přidáme další směrovač a oba propojíme pomocí sériového rozhraní. K propojení je třeba využít ikonu Add a link nebo použít pravé tlačítko myši a vybrat Add a link. 

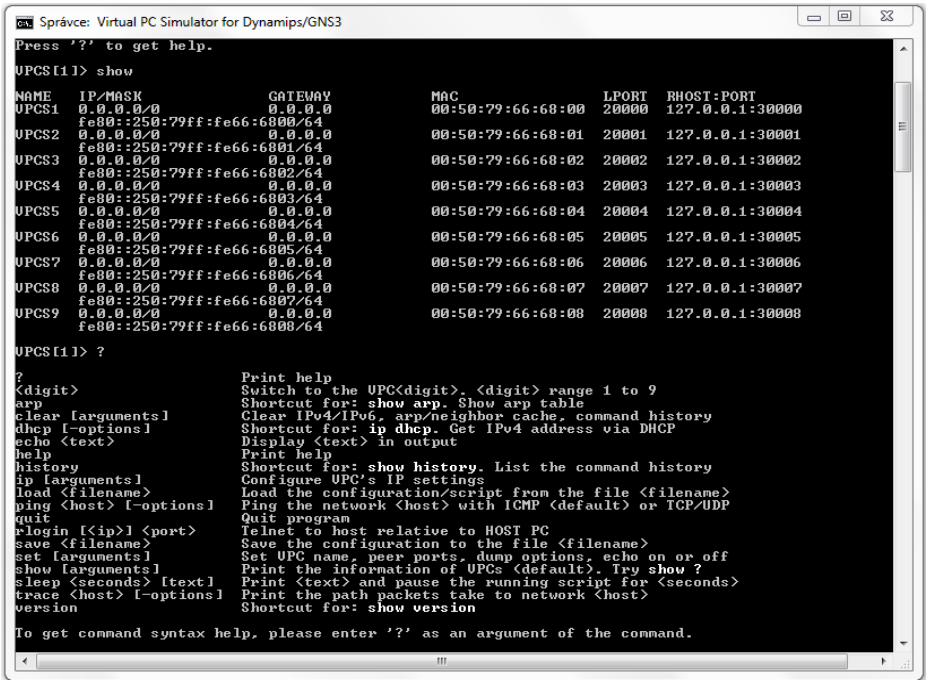
6. GNS3 obsahuje i softwarové switche a huby. Jsou to switche, na kterých neběží reálný systém jako na routerech. Tyto switche umožňují i VLANy, ale v jejich základní podobě. Je například možné nastavit každému portu switche jiný VLAN a mód. Takovým způsobem můžeme udělat libovolné množství portů. Přidáme switch na aktivní plátno výběrem ikony switche z levého pásu ikon, a zvolíme Ethernet Switch.



Obrázek 2.5: *Konfigurace switche*

7. Kromě routerů a switchů se neobejdeme bez koncových stanic. Tady máme na výběr hned z několika možností. Můžeme přidat zjednodušenou verzi stanice integrovanou v GNS3 nazvanou jako VPCS (virtuální počítače) nebo můžeme použít virtuální systém z programu VirtualBox. Následně si vyzkoušíme obě možnosti.

VPCS - z levého pásu ikon vybereme položku End Devices a přetáhneme Host na naše aktivní plátno. Tento host je přímo napojen na utilitu VPCS, kterou spustíme klinutím na Tools z hlavní nabídky a poté VPCS. Jak můžeme vidět na obrázku 2.6, tak máme k dispozici celkem 9 těchto virtuálních počítačů. Příslušný VPCS je určen svými čísly portů a unikátní MAC adresou. Jelikož se jedná o zjednodušenou koncovou stanici, můžeme provádět jen několik základních operací jako například nastavit IP adresu a masku (podpora IPv6), výchozí bránu, získávat adresu z dhcp serveru, pingovat, používat trace nebo přistoupit k jinému zařízení pomocí Telentu. Připojíme tedy VPCS1 na jeden z portů switche (musíme na ikonce Host vybrat nio_udp:30000:127.0.0.1:20000, což je právě náš VPCS1).



Obrázek 2.6: *VPCS*

VirtualBox - GNS3 umožňuje integraci VirtualBox přímo do našich topologií, avšak VirtualBox není součástí instalace a je nutné jej doinstalovat. Můžete jej zdarma stáhnout přímo ze stránek VirtualBoxu [7]. Poté co jej nainstalujete a zavedete do něj i libovolný virtuální systém, je nutné daný systém přidat do GNS3 jako hosta. Z hlavní nabídky vybereme Edit a Preferences. V okně Preferences je třeba zvolit VirtualBox a v záložce General Settings otestovat funkčnost stiskem tlačítka Test Settings (předtím si ale musíte uložit vaši topologii klavesami CTRL+S, protože testování smaže celou topologii). Tento test je třeba udělat pouze jednou, a to po bezprostřední instalaci VirtualBoxu a nebo při potížích. Pokud test proběhl v pořádku, začneme přidávat virtuální systémy do GNS3. Vybereme záložku VirtualBox Guest, jak je znázorněno na obrázku 2.7. Vyberte identifikační jméno a virtuální systém z VM List (je nutné obnovit tento seznam stiskem Refresh VM List). Pole Number of NICs určuje, kolik bude našemu virtuálnímu systému poskytnuto síťových karet.

Reserve first NIC for VirtualBox NAT to host OS - rezervuje první síťovou kartu jako konfigurovanou NATem a umožní jí přístup z virtuálního počítače na internet skrz váš hostitelský počítač, na kterém běží GNS3 (pouze pokud je k dispozici připojení).

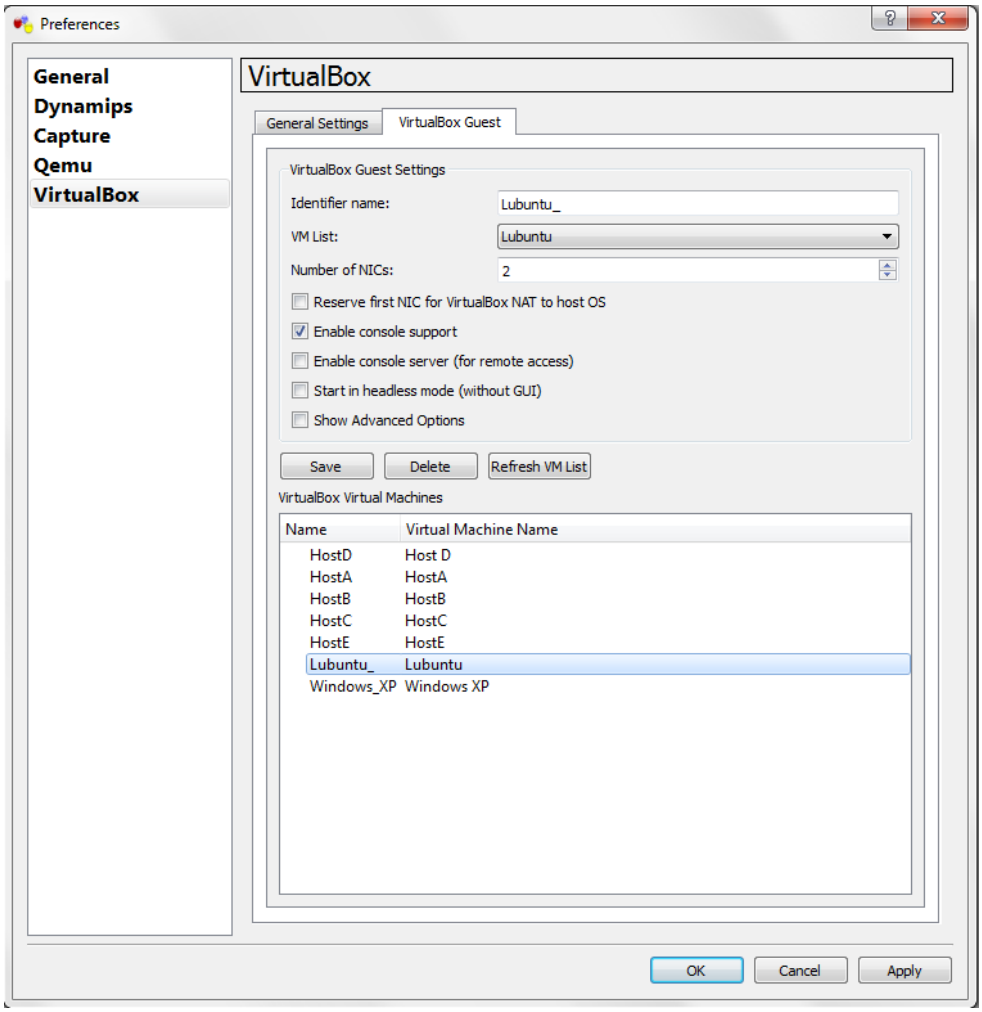
Enable console support - aktivuje přístup přes sériovou konzoli k virtuálnímu systému (musí být nakonfigurována i na straně virtuálního systému).

Enable console server - slouží pro vzdálený přístup na sériovou konzoli. GNS3 vytvoří Telnet server, který se chová jako proxy mezi sériovou konzolí a Telnet klienty.

Start in headless mode - spouští virtuální systém bez grafického rozhraní.

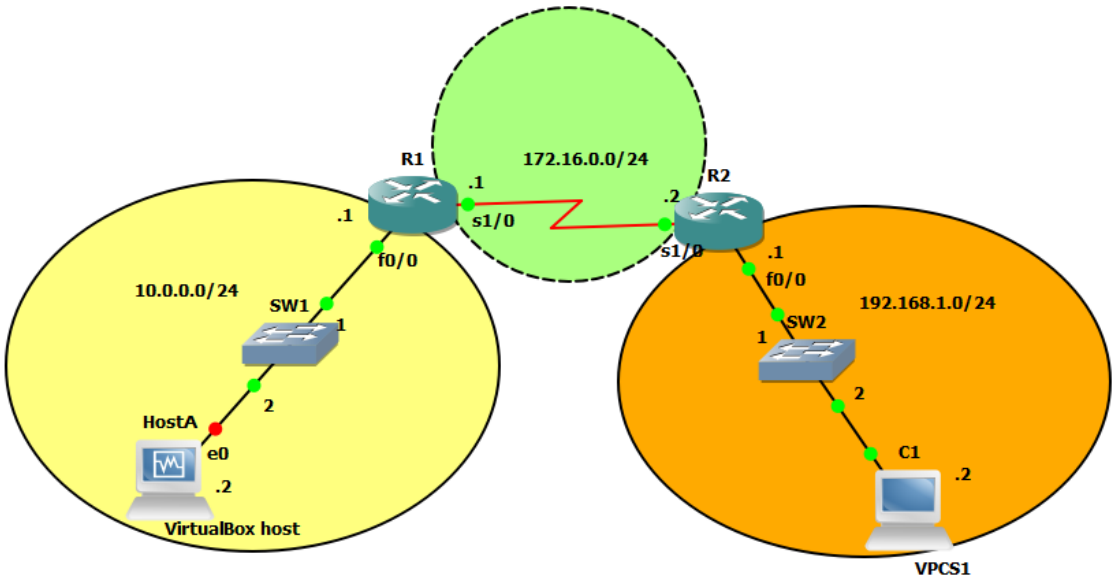
Show Advanced Options - zobrazí pokročilé možnosti př. nastavení hesla.

Pro naše účely postačí zaškrtnout pole Enable console support. Poté stiskneme tlačítko Save a nastavení virtuálního hosta uložíme. Z levého pásu ikon zvolíme ikonu koncových zařízení End Devices. Vybereme položku VirtualBox guest a z nabídky zvolíme námi přidaný virtuální systém.



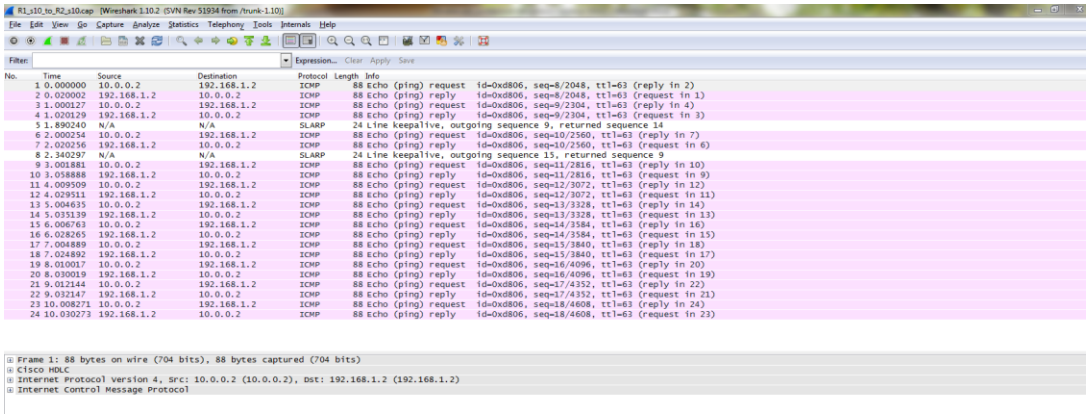
Obrázek 2.7: *VirtualBox Guest*

8. Dalším krokem je konfigurace. Spustíme všechna zařízení pomocí tlačítka Start v horním pásu ikon. Klikneme na náš směrovač R1 pravým tlačítkem myši a vybereme konzoli. Konzole se nám otevře ve výchozím terminálu Putty. Pravým klinutím na VirtualBox hosta a zvolením konzole se nám otevře konfigurační okno. Poté nakonfigurujeme naši topologii dle schématu na obrázku 2.8. Konfigurační soubory jsou dostupné v příloze Cvičení 1 Konfigurace.



Obrázek 2.8: *Topologie cvičení č. 1*

9. V programu GNS3 je integrován program Wireshark, který je součástí instalace. Pomocí Wiresharku můžeme odchytávat packety přímo na naší síti, a to na konkrétním rozhraní, které si zvolíme. Ještě než začneme odchytávat packety na naší síti, musíme zkontrolovat správné nastavení Wiresharku v programu GNS3. Přejdeme tedy v hlavní nabídce na položku Edit a vybereme Preferences. V záložce Capture a dále pod popisem Settings změníme položku Default Presets na Wireshark Traditional Capture. Potvrdíme výběr stiskem tlačítka Use. Ještě je třeba zkontrolovat výchozí cestu ke spouštěcímu souboru Wiresharku (wireshark.exe %c). Pokud je cesta správná, zaškrtneme automatické spouštění Wiresharku při zachytávání. Nyní na libovolné z našich stanic necháme neustále posílat ping na protější stanici. Samotné zachytávání packetů spustíme pravým kliknutím na příslušnou linku, v našem případě sériové rozhraní směrovače R1 a zvolíme Start capturing.



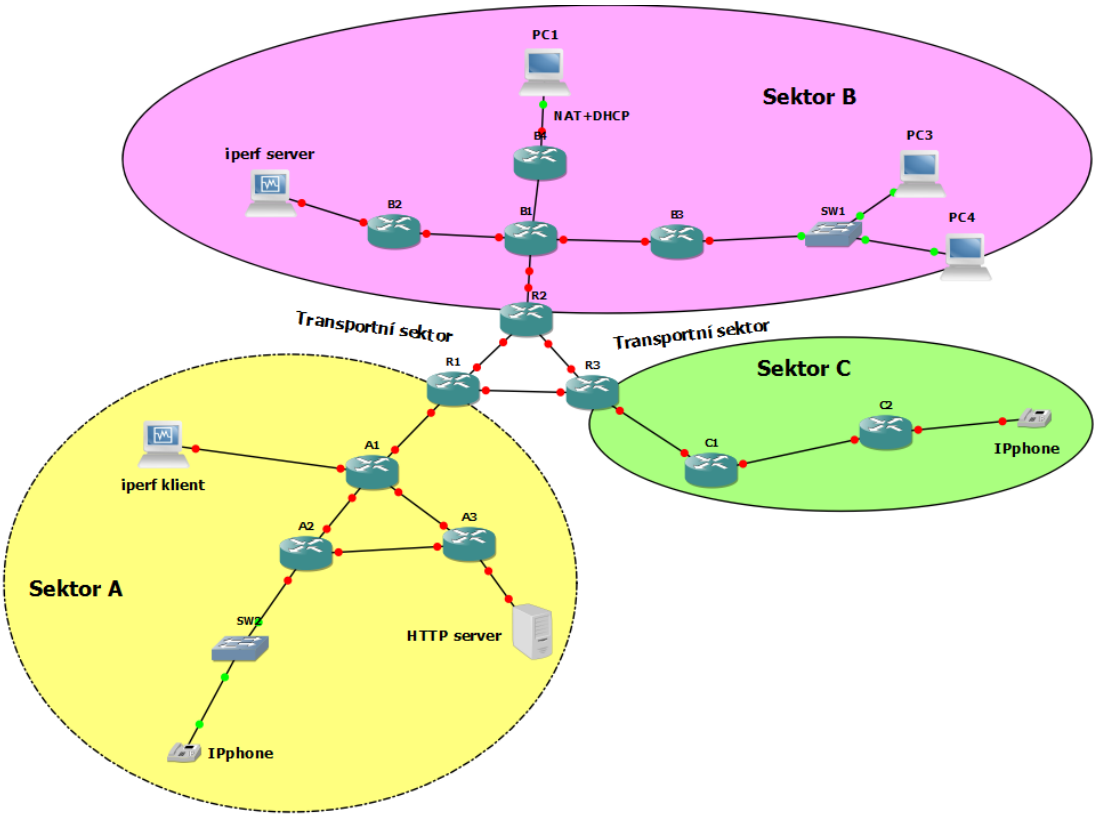
Obrázek 2.9: *Wireshark*

2.2 Cvičení číslo 2

2.2.1 Modelování počítačové sítě

Cvičení číslo dvě má komplexnější charakter a zaměřuje se na modelování počítačové sítě. Účelem tohoto cvičení je sledování chování sítě respektive provozu na síti a následné zajištění kvality určitých služeb, jako například VOIP.

1. Díky znalostem z předchozího cvičení sestavíme topologii dle obrázku 2.10. Vzorová topologie je rozdělená do čtyř sektorů. Transportní sektor je tvořen směrovači R1, R2 a R3. Sektor A obsahuje tři směrovače, jeden Ethernetový switch, jeden IP telefon a dva virtuální počítače. Sektor B je tvořen pěti směrovači, jedním Ethernetovým switchem a celkem pěti virtuálními stanicemi. Sektor C obsahuje dva směrovače a jeden IP telefon.



Obrázek 2.10: Topologie cvičení číslo 2

2. Vytvoříme si adresní plán naší topologie. Transportnímu sektoru je poskytnut adresní rozsah 172.16.0.0/24. Pro tento sektor budeme potřebovat celkem tři podsítě se čtyřmi IP adresami (2 IP + adresa sítě + broadcast). Sektoru A jsem vymezil adresní rozsah 10.0.0.0/24. Tento sektor obsahuje celkem 7 podsítí. Pět z nich obsahuje vždy 4 IP adresy a zbylé dvě 8 IP adres. Sektor B má přidělen rozsah 192.168.0.0/24. Aplikací VLSM rozdělíme tento rozsah na 7 podsítí, kde šest z nich obsahuje 4 IP adresy, a poslední sedmá 8 IP adres. Nakonec sektor C má k dispozici adresní rozsah 20.0.0.0/24. Tento sektor se skládá ze dvou podsítí o 4 IP

adresách a jedné podsítě o 8 IP adresách. V uvedených počtech IP adres podsítí jsou zahrnuty i adresy samotných sítí a broadcastů. Kompletní VLSM plán je dostupný v příloze Cvičení 2 VLSM plán.

3. Nyní přejdeme k samotné konfiguraci. Směrovač R1 je součástí transportního sektoru a zároveň tvoří výchozí cestu z/do sektoru A. Jako ukázku zde uvádím část konfigurace směrovače R1. Všechny ostatní konfigurace směrovačů jsou podobné, a proto je zde nebudu uvádět celé. Konfigurace všech prvků v síti jsou dostupné na přiloženém CD v adresáři Cvičení 2 Konfigurace.

```
conf t
#přechod do konfiguračního režimu
interface FastEthernet 0/0
#přechod na úpravu rozhraní seriál 1/0
ip address 172.16.0.9 255.255.255.252
#nastavení IP adresy a masky danému rozhraní
no shutdown
#uvedení rozhraní do režimu up
exit
#návrat do základní nabídky
router ospf 1
#nastavení směrovacího protokolu OSPF ID 1
network 172.16.0.8 0.0.0.3 area 0
#přidání sítě do routovací tabulky
exit
exit
copy running-config startup-config
#zkopíruje běžící nastavení jako nastavení při spuštění
```

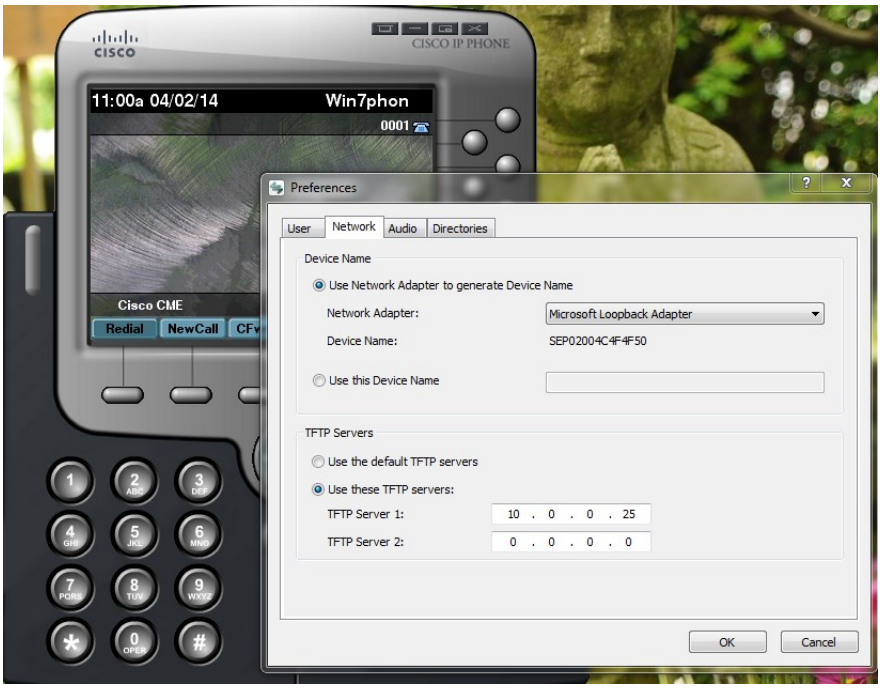
Směrovači R1 je potřeba nakonfigurovat všechna jeho rozhraní a do směrovacího protokolu OSPF zahrnout všechny sítě, ke kterým je R1 fyzicky připojen. Směrovače R2 a R3 se budou mimo jejich IP adres konfigurovat naprosto stejně. Směrovač A1 ze sektoru A má stejně jako směrovače R1-R3 nakonfigurovány všechny rozhraní a směrovací protokol OSPF. V sektoru A je zajištěn vzdálený přístup na směrovače pomocí nezabezpečené technologie Telnet. V zásadě se jedná o tuto jednoduchou konfiguraci. Nastavíme heslo pro připojení na směrovač pomocí virtuálního terminálu na „cisco“ a heslo pro přechod do enable režimu také na „cisco“.

```
conf t
enable password cisco
line vty 0 1
password cisco
login
```

Směrovač A2 je oproti ostatním směrovačům ze sektoru A obohacen o DHCP server a Telefonní službu. Funkce DHCP je úzce spjata právě s danou Telefonní službou, jelikož nechceme náš VOIP telefon neustále konfigurovat ručně. Konfigurace telefonní služby je zajištěna následovně. V konfiguračním režimu zadáme příkaz `telephony-service setup`. Poté jsme po krocích provedeni instalačním průvodcem telefonní služby. Hned jako první bod se nás průvodce dotáže, zdali chceme nakonfigurovat DHCP server. Pokud zvolíte ano, vyžaduje po vás specifikaci DHCP poolu v našem případě 10.0.0.24, dále masku podsítě pro naše DHCP, tedy 255.255.255.248. Adresu TFTP serveru pro VOIP, v našem případě 10.0.0.25 a výchozí router pro DHCP rovněž 10.0.0.25. Po základní konfiguraci služby DHCP přecházíme k samotné konfiguraci telefonní služby. Nejprve je po nás požadována zdrojová IP adresa pro Cisco IOS telefonní službu, a sice 10.0.0.25. Jako další musíme zadat port, na kterém bude telefonní služba fungovat. My necháme výchozí port 2000. Další otázkou je kolik chceme nakonfigurovat IP telefonů. Nám v této části topologie postačí jeden. Na otázku jaké telefonní číslo bude mít náš IP telefon, odpovíme 0001. Zbylé otázky pro nás nejsou důležité, a proto u nich zadáme „no“. Jako IP telefon budeme používat Cisco IP Communicator. Tento softwarový IP telefon má velkou výhodu v tom, že používá CDP protokol a jakmile jej připojíme k routeru, automaticky si zjistí veškeré potřebné informace a provede všechna nastavení sám. Jedinou nutností je ručně zadat adresu TFTP serveru. To provedeme kliknutím na horní ikonu úplně vlevo a zvolíme nabídku Preferences. V záložce Network vybereme síťový adaptér, který máme připojený do GNS3 a přepíšeme adresu TFTP serveru na 10.0.0.25 jako na obrázku 2.11. Na routeru A2 pak dodáme konfigurační příkazy upřesňující nastavení našeho IP telefonu.

```
ephone-dn 1
name Win7
description Win7phone
exit
ephone 1
keepalive 10
button 1:1
exit
dial-peer voice 2 voip
```

```
session target ipv4:20.0.0.6
destination-pattern 000.
```



Obrázek 2.11: Cisco IP Communicator

Směrovač A3 je nakonfigurován podobně jako směrovač A1 s tím rozdílem, že je mu dán větší adresní prostor 10.0.0.16/29. K tomuto směrovači je připojen náš virtuální stroj se systémem Lubuntu, na kterém běží HTTP server a Iperf. HTTP server je řešen nainstalováním balíku **apt-get install apache2**. V sektoru B máme pět směrovačů. Ke všem směrovačům v tomto sektoru je zajištěn vzdálený přístup pomocí zabezpečené služby SSH [2]. Viz konfigurace níže.

```
ip domain-name test.net
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
username admin privilege 15 secret cisco
line vty 0 4
login local
transport input ssh
exit
```

Směrovače B1-B3 jsou kromě SSH nakonfigurovány prakticky stejně jako směrovače v sektoru A. Liší se vždy pouze IP adresy a jejich rozhraní. Směrovače B4 a B5 mají nakonfigurován překlad adres NAT a službu DHCP. Uvedu tedy ukázku konfigurace NATu.

Kromě vytvoření přístupového seznamu a jeho překladu je nutné přesně specifikovat, které rozhraní bude vnitřní a které vnější.

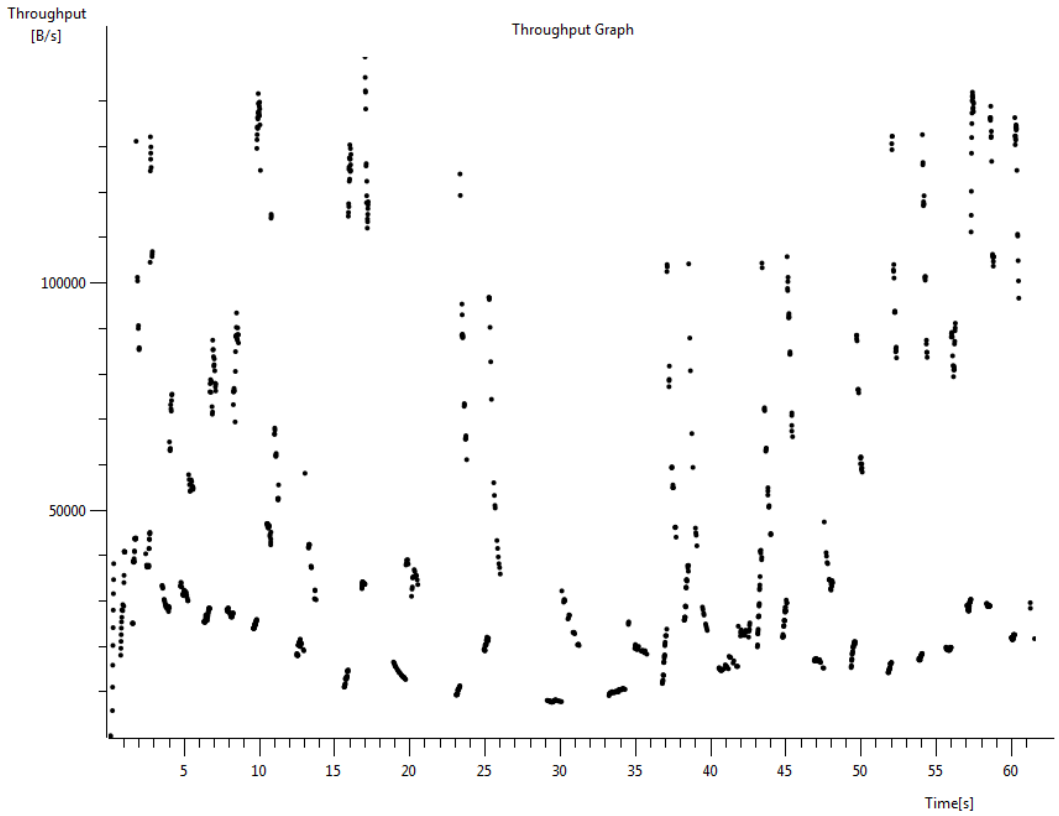
```
interface fastEthernet 0/0
ip nat outside
int fa 0/1
ip nat inside
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface fastEthernet 0/0 overload
exit
```

V sektoru B je dále jeden virtuální stroj se systémem Linux Microcore, na kterém běží Iperf (generátor provozu na síti). Další stroj se systémem Lubuntu budeme používat pro zobrazení webových stránek na http serveru ze sektoru A. V sektoru C jsou pouze dva směrovače. C1 je pouze jako průchozí a na C2 je nakonfigurována Telefonní služba podobným způsobem jako na směrovači A2. Jediný rozdíl je v pojmenování IP telefonu a v telefonním čísle, které je 0002. Na virtuálním stroji v sektoru C je pak nainstalován systém Windows XP. Na tomto systému používáme stejný software jako v sektoru A, a sice Cisco IP Communicator.

4. Nyní přejdeme k samotnému modelování provozu na této síti. Nejdříve je třeba zjistit, jak se síť chová, když je zatížena nějakým provozem. Nejvhodnějším základním nástrojem pro síťový monitoring je příkaz ping. Pingem si ověříme dostupnost všech síťových prvků v naší architektuře, včetně serverů.

5. Pokud všechny síťové prvky odpovídají na příkaz ping, vyzkoušíme test propustnosti. K tomuto účelu použijeme program Iperf nainstalovaný na našich virtuálních strojích se systémem Linux, který bude generovat TCP packety mezi klientem v sektoru A, a serverem v sektoru B. Na straně serveru aktivujeme Iperf zadáním příkazu `iperf -s`. Tímto spustíme Iperf server, který je připraven naslouchat na výchozím portu 5001 a adrese 192.168.0.22. Na straně klienta pak zadáme příkaz `iperf -c 192.168.0.22 -P 2 -t 80`, který nám říká, že spouštíme Iperf jako klienta a připojujeme se k serveru na adrese 192.168.0.22. Iperf nám nyní bude generovat dva tcp packetové streamy po dobu 80 sekund [3]. Necháme Iperf běžet a zároveň uskutečníme telefonní hovor z IP telefonu ze sektoru C na IP telefon ze sektoru A. Na IP telefonu zavoláme telefonní číslo 0002.

6. Nyní nám běží provoz a je nutné jej analyzovat. K tomu použijeme program Wireshark. Klikneme pravým tlačítkem na nejvytíženější linku, v našem případě rozhraní seriál 1/0 směrovače R1 a zvolíme Capture. Poté co Iperf test skončí, zastavíme i zachytávání packetů. Klikneme na libovolný TCP packet a vybereme z menu Statistics volbu TCP Stream Graph a Throughput Graph. Tento graf nám ukazuje propustnost TCP packetů v čase.



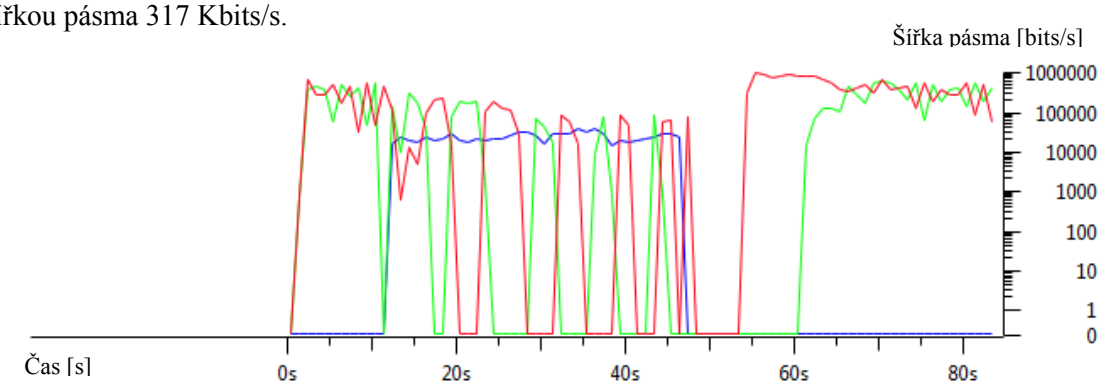
Obrázek 2.12: Wireshark TCP Throughput

Z obrázku [2.12] je patrné, že propustnost TCP packetů velice kolísala. To je částečně způsobeno i vlastnostmi GNS3. Tento typ grafu ukazuje pouze propustnost jednoho TCP streamu v jednom směru, ze sektoru A, do sektoru B. Větší přehled o tom, jak se chovala naše síť, si můžeme ukázat na obrázku [2.13]. Graf na tomto obrázku vygenerujeme pomocí nabídky Statistics, ale tentokrát vybereme položku IO Graph. Tento graf nám zobrazuje závislost využité šířky pásma daného rozhraní na čase. Jednotlivý provoz je třeba rozlišit použitím filtrace. Zeleně vyznačíme TCP stream na portu 53298. Červeně je vyznačen TCP stream na portu 53299. Modře je nakonec vyznačen RTP stream, tj. provoz, který je zodpovědný za přenos telefonní služby VOIP. RTP stream potřebuje pro provoz jednoho hovoru šířku pásma zhruba 80 Kbits/s. V rámci simulace zatížení sítě byla šířka pásma pro jeden simulovaný hovor více než dostačující, proto křivka RTP streamu nijak nekolísá a udržuje si konstantní propustnost. Naopak oba TCP streamy zaznamenávají zvýšené kolísání propustnosti právě během probíhajícího hovoru. Program GNS3 neumožňuje ovlivňovat nastavení šířky pásma jednotlivých rozhraní. GNS3 nebere v úvahu fyzickou vrstvu, a tudíž je celková šířka pásma dána výkonem našeho počítače, na kterém program GNS3 běží. Pro srovnání na mém osobním počítači s dvoujádrovým procesorem Intel E8400 s frekvencí 3.00 GHz a 4 GB paměti RAM jsem dosahoval maximální propustnosti něco kolem 600 Kbits/s. Výpis z programu Iperf a dosažená propustnost (šířka pásma) viz níže.

```
[  4]  0.0-80.3 sec  1.95 MBytes    203 Kbits/sec
```

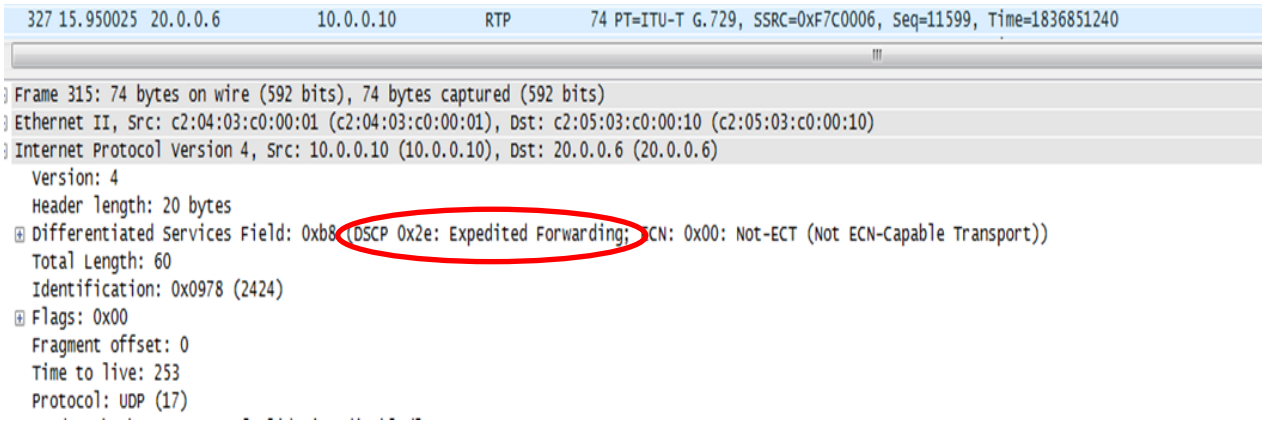
```
[  3]  0.0-81.0 sec  1.12 MBytes    116 Kbits/sec
[SUM]  0.0-81.0 sec  3.06 MBytes    317 Kbits/sec
```

Pod číslem 4 je první TCP stream, který odeslal celkem 1,95 MBytů dat s dosaženou šířkou pásma 203 Kbits/s. Pod číslem 3 je druhý TCP stream, který odeslal 1,12 MBytů dat a dosáhl šířky pásma 116 Kbits/s. Sumárně bylo tedy přeneseno 3,06 MBytů dat s dosaženou šířkou pásma 317 Kbits/s.



Obrázek 2.13: Wireshark I/O Graph

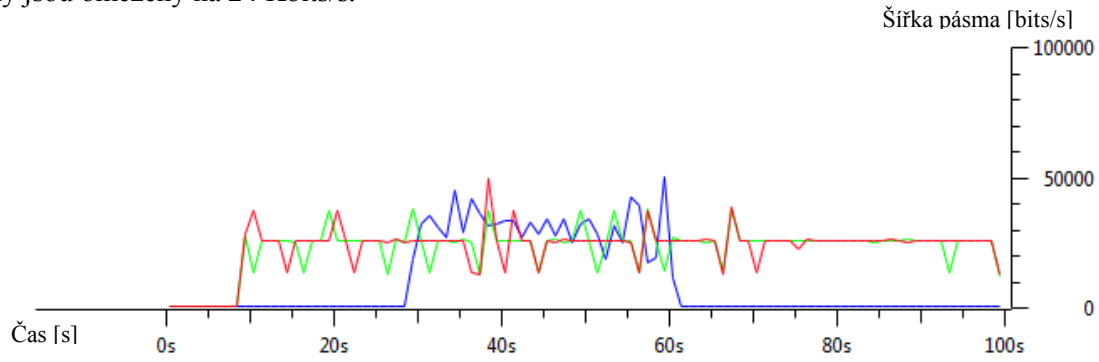
7. Nyní víme, jak se chová naše síť při zátěži. Abychom přiblížili toto cvičení reálné situaci, aplikujeme v naší síti QoS (kvalita služeb). V praxi platí pravidlo, že telefonní služba by měla mít určitou garanci šířky pásma. Toto učiníme i v rámci našeho cvičení. Jelikož GNS3 nereaguje na nastavení šířky pásma na lince, budeme uvažovat o linkách se šířkou pásma 100 Kbits/s. Hovorové službě VOIP, která ke svému přenosu využívá RTP packety garantujeme prioritně 65 % šířky pásma. Na směrovači A2 musíme vytvořit třídní mapu VOIP (class-map VOIP), která bude přijímat protokol RTP. Poté vytvoříme politiku HLAS (policy-map HLAS), v níž pro třídní mapu VOIP nastavíme hodnotu DSCP (differentiated service code point) na EF (expedited forwarding), což je hodnota pro real-time provoz s nízkým zpožděním. Nakonec tuto politiku aplikujeme jako vstupní na rozhraní FastEthernet 0/0 směrovače A2. RTP packety, které teď dorazí na rozhraní FastEthernet 0/0 směrovače A2 budou označeny hodnotou DSCP EF. Tyto označené packety zpracujeme na směrovači A1, kde nastavíme třídní mapu tak, aby snímala označené packety. V politice směrovače A1 pak těmto nasnímaným packetům přiřadíme prioritu 65% z celkové šířky pásma. Tuto politiku pak nastavíme jako výstupní na rozhraní FastEthernet 0/1 směrovače A1. Takto postupujeme na každém dalším směrovači, po kterém by eventuálně hovor mohl probíhat. Nyní si ověříme, zdali opravdu GNS3 umí packety označit. Iniciujeme hovor z jednoho terminálu na druhý a odchytíme si packety pomocí Wiresharku. Jak vidíme na obrázku [2.14], packety jsou opravdu označeny hodnotou DSCP Expedited Forwarding [4].



Obrázek 2.14: Differentiated service code point

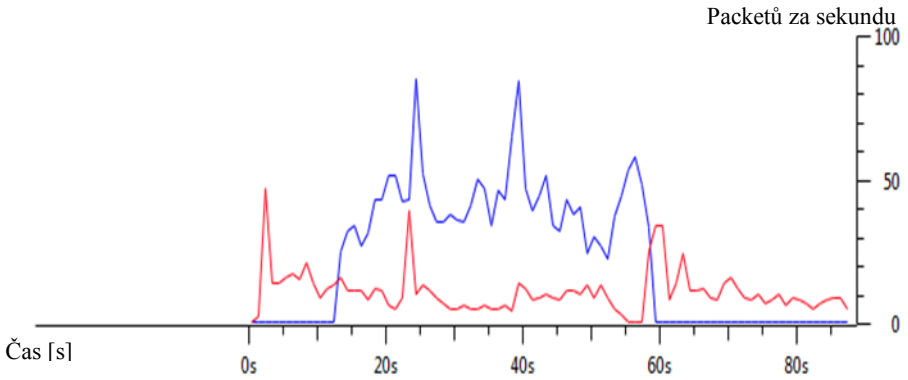
V rámci aplikování kvality služby použijeme i funkci modelování (shape). Budeme modelovat všechen ostatní provoz, tj. ten který není RTP. Do toho provozu bude spadat i TCP stream generovaný programem Iperf. Jelikož uvažujeme šířku pásma 100 Kbits/s a hovorové službě garantujeme 65 %, mělo by pro ostatní provoz zbýt 35%. Tak tomu ale není, protože GNS3 neakceptuje šířku pásma nastavenou na směrovačích. Proto použijeme funkci shape. Do politiky, která je už aplikována na směrovačích jako výstupní přidáme výchozí třídu (class-default) a vytvarujeme její šířku pásma na konstantních 24 Kbits/s. Tím zároveň zabráníme různým kolísáním šířky pásma a docílíme toho, že veškerému provozu mimo RTP stream bude nastavena napevno šířka pásma 24 Kbits/s.

8. Máme nastavenou kvalitu služby QoS. Opět provedeme zatížení sítě a zjistíme, jak se změnilo její chování. Zachytíme si provoz Wiresharkem a vytvoříme I/O Graph z menu Statistics. Vyfiltrujeme RTP provoz a TCP streamy. Na obrázku [2.15] je modře vyznačen RTP stream, červeně TCP stream na portu 53299 a zeleně TCP stream na portu 53298. Z analýzy jde jasně vidět, že RTP stream opravdu využívá 65% z celkové šířky pásma 100 Kbits/s. Jelikož nejde nastavit šířka pásma na rozhraních směrovačů v GNS3, tak nedochází během probíhajícího hovoru k výraznému snížení propustnosti TCP streamů. Naproti tomu je jasně vidět, že funkce tvarování průběhů (modelování) v GNS3 opravdu funguje. Vidíme, že oba TCP streamy jsou omezeny na 24 Kbits/s.



Obrázek 2.15: Chování sítě po aplikaci QoS

Na obrázku [2.16] je znázorněn počet prošlých packetů za sekundu. Modře RTP stream a červeně oba TCP streamy dohromady. Modrých packetů v době od 10 sekundy do 60 sekundy prošlo mnohem více než červených. To je dáno tím, že jsme RTP provozu nastavili určitou prioritu, a tudíž má přednost před čímkoliv jiným.



Obrázek 2.16: Množství packetů za sekundu

9. Závěrem cvičení 2 zhodnotíme naměřené výsledky. Při běžném zatížení sítě docházelo k velkému kolísání obou streamů jak TCP, tak RTP. Největší kolísání TCP streamu probíhalo právě při probíhajícím hovoru. Toto chování jsme upravili aplikací kvality služby QoS. Hovorová služba je pro nás prioritní a nastavili jsme ji také prioritu 65% šířky pásma. TCP streamům jsme nastavili tvarování na 24 Kbits/s abychom zabránili výkyvům. Provoz jsme znovu zachytili a analyzovali. RTP packety byly označeny příznakem na třetí vrstvě modelu OSI DSCP hodnotou. Při zobrazení I/O Grafu ve Wiresharku bylo jasně vidět i úspěšné tvarování na 24 Kbits/s. Tomu, že má RTP stream prioritní práva, odpovídal i graf zobrazující počet prošlých packetů za sekundu. RTP packetů prošlo více.

Závěr

Ve své bakalářské práci jsem prezentoval jednu z mnoha alternativ pro simulace počítačových sítí, a sice program GNS3. GNS3 je zcela zdarma, a to si považuji za jednu z velkých výhod. Vzhledem ke zkušenostem, které jsem během jeho používání nabral, bych tento nástroj doporučil opravdu každému studentovi či jinému uživateli, který potřebuje jednoduše a rychle simulovat nějakou síťovou situaci či pouze otestovat funkčnost konfigurace. Naproti tomu složitější simulace jsou velice náročné na výpočetní výkon počítače, na kterém GNS3 provozujeme. Jedna z vlastností GNS3 je, že nelze ovlivnit šířku pásma na rozhraních směrovačů. Šířka pásma je v GNS3 daná výkonem PC. Právě kvůli této vlastnosti nelze očekávat reálné výsledky při prováděných testech propustnosti. Na počítači s dvoujádrovým procesorem s frekvencí 3.00 GHz a pamětí RAM o velikosti 4 GB jsem dosahoval propustnosti maximálně 680 Kbits/s. Když však vezmeme v úvahu tyto vlastnosti, můžeme si vytvořit náhled a provádět tak téměř jakékoliv síťové situace a následně provést korekci naměřených dat. Díky tomu pak získáme smysluplnější výsledky vztažené k reálným situacím.

Podařilo se mi vytvořit dvě zadání pro laboratorní cvičení z odborného předmětu. Tyto cvičení budou v závislosti na rozhodnutí mého vedoucího práce Ing. Libora Michalka Ph.D. použity právě na hodinách jeho předmětu Modelování počítačových sítí. Zadání těchto cvičení jsou koncipována tak, aby studenti za krátkou dobu pochytili co nejvíc zkušeností v oblasti práce s programem GNS3 a modelování sítí. První cvičení je zaměřeno na práci s programem a jeho pokročilé funkce. Druhé cvičení je zaměřeno na modelování sítě, analýzu provozního zatížení a aplikaci kvality služeb QoS. I přes nemožnost ovlivnit fyzickou vrstvu na úrovni rozhraní směrovačů funguje QoS velice dobře. GNS3 je v neustálém vývoji a jeho vývojáři přidávají nové funkce. V budoucnosti se můžeme dočkat dokonce i podpory přepínání (switchingu).

Použitá literatura

[1] GNS3. Hardware emulated by GNS3. *GNS3: Graphical Network Simulator* [online]. [cit. 2014-04-26]. Dostupné z: http://www.gns3.net/hardware-emulated/

[2] SOUNDTRAINING.NET. Soundtraining.net: IT Tutorials. *Soundtraining.net: accelerated i.t. training* [online]. [cit. 2014-04-28]. Dostupné z: http://www.soundtraining.net/i-t-tutorials/cisco-tutorials/31-cisco-router-ssh-configuration

[3] ŠTRAUCH, A. Iperf: Měření rychlosti spojení. In: *ROOT.cz* [online]. [cit. 2014-04-28]. Dostupné z: http://www.root.cz/clanky/iperf-mereni-rychlosti-spojeni/

[4] GNS3Vault: QUALITY OF SERVICE (QOS). *GNS3Vault: Free Cisco Labs for CCNA, CCNP and CCIE R&S!* [online]. [cit. 2014-04-28]. Dostupné z: http://gns3vault.com/Labs/Quality-of-Service-QOS/

[5] WELSH, Ch. Dynamips/GNS3 Idle-PC explained. Finally!. In: *RedNectar's Blog* [online].[cit.2014-04-28]. Dostupné z: http://rednectar.net/2013/02/24/dynamipsgns3-idle-pc-explained-finally/

[6] GNS3. Documentation. *GNS3: Graphical Network Simulator* [online]. [cit. 2014-04-29]. Dostupné z: http://www.gns3.net/documentation/

[7] ORACLE. *VirtualBox* [online]. [cit. 2014-04-29]. Dostupné z: https://www.virtualbox.org/

Seznam příloh

Součástí BP je CD.

Adresářová struktura přiloženého CD/DVD:

Cvičení 2 Konfigurace

Bakalářská práce.pdf

Příloha A: *Seznam podporovaného hardwaru*

Cisco 1700 Series

1700 série má jednu a více rozhraní na základní desce, 2 subsloty pro WAN karty rozhraní(WIC) a žádné NM sloty.

1710

- 1 FastEthernet a 1 Ethernet napevno nastaven (CISCO1710-MB-1FE-1E).
- WIC sloty: 0

1720**,** 1721 **a** 1750

- 1 FastEthernet napevno nastaven (C1700-MB-1ETH).
- WIC sloty: 2 (maximálně 2x Ethernet nebo 4x Serial).

1751 **a** 1760

- 1 FastEthernet napevno nastaven (C1700-MB-1ETH).
- WIC sloty: 2 (maximálně 2x Ethernet nebo 4x Serial).

WIC karty

- WIC-1T (1 sériový port)
- WIC-2T (2 sériové porty)
- WIC-1ENET (1 Ethernet port)

Cisco 2600 Series

2600 má jedno nebo více rozhraní na základní desce, 2 subsloty pro WIC karty a 1 síťový modul NM.

2610

- 1 Ethernet napevno (CISCO2600-MB-1E).
- NM sloty: 1 (maximálně 4 Ethernet porty nebo 16 FastEthernet portů).
- WIC slots: 3 (maximálně 6 sériových portů).

2611

- 2 Ethernet napevno (CISCO2600-MB-2E).
- NM sloty: 1 (maximálně 4 Ethernet porty nebo 16 FastEthernet portů).
- WIC slots: 3 (maximálně 6 sériových portů).

2610XM, 2620, 2620XM a 2650XM

- 1 FastEthernet napevno (CISCO2600-MB-1FE).
- NM sloty: 1 (maximálně 4 Ethernet porty nebo 16 FastEthernet portů).
- WIC sloty: 3 (maximálně 6 sériových portů).

2611XM, 2621, 2621XM and 2651XM

- 2 Ethernet napevno (CISCO2600-MB-2FE).
- NM sloty: 1 (maximálně 4 Ethernet porty nebo 16 FastEthernet portů).
- WIC slots: 3 (maximálně 6 sériových portů).

Síťové moduly NM

- NM-1E (1 Ethernet port)
- NM-4E (4 Ethernetové porty)
- NM-1FE-TX (1 FastEthernet port)
- NM-16ESW (switch modul: 16 FastEthernet portů)

- NM-NAM (Network Analysis Module, zatím nefunguje v GNS3).
- NM-IDS (IDS Network Module, zatím nefunguje v GNS3).

WIC karty

- WIC-1T (1 sériový port)
- WIC-2T (2 sériové porty)

Cisco 3600 Series

3600 má 2-6 Síťových modulů (NM).

3620

- NM sloty: 2 (maximálně 8 Ethernetových portů, 32 FastEthernet portů nebo 8 sériových portů).

3640

- NM sloty: 4 (maximálně 16 Ethernetových portů, 32 FastEthernet portů nebo 16 sériových portů).

3660

- 2 FastEthernet napevno (Leopard-2FE).
- NM sloty: 6 (maximálně 24 Ethernetových portů, 32 FastEthernet portů nebo 24 sériových portů).

Síťové moduly NM

- NM-1E (1 Ethernet port)
- NM-4E (4 Ethernetové porty)
- NM-1FE-TX (1 FastEthernet port)
- NM-16ESW (switch modul: 16 FastEthernet portů, maximálně dva tyto moduly pro router)
- NM-4T (4 sériové porty)

Cisco 3700 Series

3700 má 2 FastEthernet rozhraní na základní desce, 3 subsloty pro WIC karty a 1-4 Síťových modulů (NM).

2691

- 2 FastEthernet napevno (GT96100-FE)
- NM sloty: 1 (maximálně 16 FastEthernet portů nebo 4 sériových portů).
- WIC sloty: 3 (maximálně 6 sériových portů).

3725

- 2 FastEthernet napevno (GT96100-FE)
- NM sloty: 1 (maximálně 32 FastEthernet portů nebo 8 sériových portů).
- WIC sloty: 3 (maximálně 6 sériových portů).

3745

- 2 FastEthernet napevno (GT96100-FE)
- NM sloty: 4 (maximálně 32 FastEthernet portů nebo 16 sériových portů).
- WIC sloty: 3 (maximálně 6 sériových portů).

Síťové moduly

- NM-1FE-TX (1 FastEthernet port)

- NM-16ESW (switch modul: 16 FastEthernet portů, maximálně dva tyto moduly pro router)
- NM-4T (4 sériové porty)
- NM-NAM (Network Analysis Module, zatím nefunguje v GNS3).
- NM-IDS (IDS Network Module, zatím nefunguje v GNS3).

WIC karty

- WIC-1T (1 sériový port)
- WIC-2T (2 sériové porty)

Cisco 7200 Series

7200 má rozdílnou architekturu. Pouze typ 7206 je podporován v GNS3 a má 6 portových adaptérů (PA).

7206

- PA sloty: 6

Chassis typy

- STD
- VXR

Network Processing Engines **(NPE)**

- NPE-100
- NPE-150
- NPE-175
- NPE-200
- NPE-225
- NPE-300
- NPE-400
- NPE-G2

Input/Output Controllers

Mohou byt vloženy pouze do slotu 0.

- C7200-IO-FE (1 FastEthernet port)
- C7200-IO-2FE (2 FastEthernet porty)
- C7200-IO-GE-E (1 GigabitEthernet port)

Portové Adaptéry

Online Insertion and Removal (OIR)funkce je podporována a umožňuje nám nahradit PA adaptéry zatímco router běží.

- PA-FE-TX (1 FastEthernet port)
- PA-2FE-TX (2 FastEthernet porty)
- PA-4E (4 Ethernetové porty)
- PA-8E (8 Ethernetových portů)
- PA-4T+ (4 sériové porty)
- PA-8T (8 sériových portů)
- PA-A1 (1 ATM port)
- PA-POS-OC3 (1 Packet-Over-SONET port)
- PA-GE (1 GigabitEthernet port)

Cisco PIX firewally
Speciální verze QEMU nazvaná PEMU je rozšířena v GNS3 pro emulaci PIX 525 Security Appliance. Je podporován PIX software ve verzi 7.2(4).

Cisco ASA firewally
Qemu/GNS3 emuluje ASA5520 (ASA 5520 Series Adaptive Security Appliance) hardware ke spuštění ASA softwaru ve verzi 8.0(2).

Cisco IDS sensors
Qemu/GNS3 emuluje IDS 4235/4215 Sensor. Software IPS je možno spustit ve vydání 6.0.

Juniper směrovače
JunOS, operační systém Juniper směrovačů je založen na architektuře FreeBSD, což je UNIX operační systém, který běží na PC. Momentálně v GNS3 funguje JunOS ve verzi Juniper M.

Host stanice
Díky VirtualBoxu a QEMU je možné spustit širokou škálu operačních systémů jako koncové stanice v GNS3. GNS3 proto vytvořilo speciální appliance, které nevyžadují mnoho paměti RAM a jsou méně náročné na výkon PC. Mezi tyto aplikace patří Linux Microcore nebo Linux Tinycore a podporují následující funkce:

- Podpora IPv6
- iperf, tcpdump, iproute2 a iptables
- SSH a telnet servery
- D-ITG (Distributed Internet Traffic Generator)

Příloha B: *Cvičení 1 Konfigurace*

Směrovač R1

```
configure terminal
interface serial 1/0
ip address 172.16.0.1 255.255.255.0
no shutdown
interface fastEthernet 0/0
ip address 10.0.0.1 255.255.255.0
no shutdown
ip route 192.168.1.0 255.255.255.0 172.16.0.2
```

Směrovač R2

```
configure terminal
interface serial 1/0
ip address 172.16.0.2 255.255.255.0
no shutdown
interface fastEthernet 0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
ip route 10.0.0.0 255.255.255.0 172.16.0.1
```

Konfigurace VPCS 1

```
ip 192.168.1.2 255.255.255.0 192.168.1.1
ping 192.168.1.1
```

Konfigurace VirtualBox hosta

```
sudo su
ifconfig eth0 10.0.0.2 netmask 255.255.255.0
route add default gw 10.0.0.1
ping 10.0.0.1
```

Příloha C: *Cvičení 2 VLSM plán*